Confidencialidad de las comunicaciones en Sistemas Móviles

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1;3]; García, Edith[1], Liporace, Julio[1]; Maiorano, Ariel[1]; Malvacio, Eduardo[1]; Tapia, Néstor[1];

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática. Escuela Superior Técnica, Facultad del Ejército. Universidad de la Defensa Nacional UNDEF.
[2] CISTIC/FCE - Universidad de Buenos Aires.
[3] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar,
{edithxgarcia; jcliporace; maiorano; edumalvacio; tapianestor87}@gmail.com

RESUMEN.

El objetivo de este proyecto es el diseño y desarrollo de un ***Algoritmo de Cifrado*** que permita dotar de confidencialidad a la información transmitida en *Sistemas Móviles.* Un algoritmo así requiere satisfacer requerimientos de robustez, compactibilidad y velocidad tales que le permitan desenvolverse con eficiencia.
Además de los resultados teóricos y prácticos, el proyecto persigue la realización de un desarrollo experimental.
Desde la mismísima etapa de diseño los algoritmos criptográficos deben demostrar su resistencia a los ataques conocidos. Es por ello que existen instancias y funciones que deben probar su resistencia a tal o cual ataque. En particular a la enorme cantidad de nuevas y poderosas herramientas de Criptoanálisis que se han desarrollado en los últimos tiempos.

Palabras Clave:

Criptografía. Criptoanálisis, Criptosistemas de Clave Privada, Stream Ciphers. Sistemas Móviles.

CONTEXTO.

En el marco de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Teleinformática que se dictan en la *Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST)*, dependiente de la *Facultad del Ejército, Universidad de la Defensa Nacional (UNDEF)* se llevan adelante tareas de I+D+i por parte del *Grupo de Investigación en Criptología y Seguridad Informática (GICSI).* El mismo depende del *Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab)* perteneciente al *Laboratorio Informática (InforLab).* Y está conformado por docentes investigadores, profesionales técnicos y alumnos de dicha área.

1. INTRODUCCIÓN.

Los sistemas "fijos" de comunicaciones disponen de mayores recursos de Hardware y Software que sus pares "móviles". Estos últimos permiten la realización de comunicaciones en posiciones fijas, como también en movimiento (por ejemplo sistemas de tipo VHF[1] entre otros). Sus capacidades de almacenamiento y procesamiento (entre otras) pueden resultar fácilmente sacrificables y ser disminuidas en beneficio de una mayor movilidad, menor peso y consumo energético, entre otras limitaciones que pudieren tener.
Sin embargo, la confidencialidad de los enlaces no puede ni debe ser reducida o eliminada por los diseñadores, fabricantes o usuarios de estos equipos en persecución de una mayor libertad de movimientos. Ello implica el pago de un alto precio al atentar contra la seguridad de la comunicación.

[1] Very High Frequency: rango de frecuencias de 30 MHz a 300 MHz. Empleado por sistemas satelitales, televisión, radiodifusoras de FM, bandas aéreas y marítimas, entre otras.

La Criptografía tiene en su haber multiplicidad de algoritmos robustos y confiables. Lamentablemente no todos ellos pueden implementarse de manera eficaz y segura en Sistemas Móviles debido a la reducción de recursos con las que funcionan: un algoritmo podría demandar una cantidad de recursos (tiempo de ejecución, energía, memoria, potencia de cálculo, etc.) que el sistema sería incapaz de suministrar. Incluso asumiendo la posibilidad que pudiera hacerlo, tal vez su ejecución podría comprometer la velocidad del sistema provocando demoras y demás efectos negativos sobre la comunicación.

En esta dirección y en el ámbito de las fuerzas armadas argentinas, CriptoLab ha realizado algunas propuestas. En especial para vehículos aéreos no tripulados del Proyecto LIPAM[1] del Ejército Argentino, los cascos de realidad aumentada del Proyecto[2] RAIOM[2] del Centro de Investigaciones para la Defensa - CITEDEF[3]. También se pueden mencionar otros sistemas y vehículos militares, como el PANHARD[3] francés que el Ejército y otras fuerzas poseen y que le fue encomendado a la EST para su modernización.

Cabe aclarar que en el ámbito civil también existen dispositivos y vehículos que requieran cifrado de características similares. Es por ello que el estudio de dichos sistemas redunda en un beneficio dual: civil y militar.

El diseño e implementación de un criptosistema reducido, veloz y económico en el consumo de recursos sería indispensable para dotar de confidencialidad a datos y canales de comando y control.

A su vez investigar sobre la existencia de problemas que generan debilidades en el cifrado. Como así también someter al sistema a los ataques criptoanalíticos reconocidos como el Criptoanálisis Diferencial, Lineal, Algebraico, Cube Attack, entre otros [4-7].

[2] RAIOM: Realidad Aumentada para la Identificación de Objetivos Militares.

[3] CITEDEF: El Instituto de Investigaciones Científicas y Técnicas para la Defensa; ex Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas (CITEFA)

2. LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN.

Hemos dividido el proyecto en 4 etapas de investigación y desarrollo:

a) Estudio y análisis de algoritmos que satisfacen los requerimientos y condiciones de entorno del proyecto.

b) Personalización, diseño y desarrollo del algoritmo:

- Estudio de sus vulnerabilidades y ataques conocidos.
- Implementación y pruebas del algoritmo.

c) Determinación de las propiedades criptológicas:

- Estudio de las propiedades.
- Experiencias de laboratorio.

d) Ejecución de los tests y demás pruebas de robustez criptológica.

- Diseño y programación de los tests.
- Diseño e implementación de los ataques.
- Análisis de los resultados obtenidos.
- Redacción del informe final.
- Puesta a punto del algoritmo a entregar.

3. RESULTADOS Y OBJETIVOS.

Se espera realizar el diseño de un esquema de cifrado y descifrado del tipo Stream Cipher (cifrado en flujo o cadena de bits) de Clave Privada, que pueda garantizar la seguridad de las comunicaciones sobre uno o más canales de comunicaciones de un Sistema Móvil.

Su fortaleza se podrá observar a través de sus propiedades matemáticas pertinentes. Además, la Secuencia Cifrante (Key Bit Stream) [8] que se obtenga, deberá satisfacer todos los requisitos aceptados por la comunidad científica que deben tener las Secuencias Seudo-Aleatorias: Test de Golomb, de NIST, Die Hard y demás, estudio de la longitud de recursión, complejidad lineal y período[9].

La realización de un desarrollo propio y nacional redundará en ahorrar recursos económicos enfrentados a los altos costos en equipos y algoritmos adquiridos en el exterior y pagaderos en moneda foránea.

4. FORMACIÓN DE RECURSOS HUMANOS.

Los docentes investigadores participantes del proyecto dictan las asignaturas *Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación I, II.* Desde esas cátedras se invita a los alumnos a participar en los proyectos de investigación. Es por ello que los alumnos *Dorado, Mariano, Cabrera Ezequiel, Leiras Facundo y Romero, Luciano* han demostrado su interés y se han sumado en calidad de colaboradores. En particular los dos últimos serán postulantes para la beca "Estímulo a las Vocaciones Científicas" (EVC) otorgadas por el Consejo Interuniversitario Nacional (CIN) por encuadrarse en las condiciones pedidas [10].

Se desea destacar que el incremento del Know-How que tendrá el grupo de investigadores a lo largo de la vida del proyecto será una importante y económica Formación de Recursos Humanos en beneficio de sus integrantes.

Atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

[1] https://es.wikipedia.org/wiki/Lip%C3%A1n_M3 consultada el 12/3/2018.

[2] http://www.historialprensa.mindef.gov.ar/articles/ver/120. consultada el 14/3/2017.

[3] Ding C.; *The differential cryptanalysis and design of natural stream ciphers*. In: Anderson R. (eds.) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol. 809. Springer Berlin, Heidelberg.

[4] https://es.wikipedia.org/wiki/Panhard_AML consultada el 14/3/2018.

[5] Wu H., Preneel B. *Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy*. In: Naor M. (eds.) Advances in Cryptology. EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515. Springer Berlin, Heidelberg. 2007.

[6] Muller F., Peyrin T. *Linear Cryptanalysis of the TSC Family of Stream Ciphers.* In: Roy B. (eds.) Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 3788. Springer, Berlin, Heidelberg. 2005.

[7] Dinur I., Shamir A. *Cube Attacks on Tweakable Black Box Polynomials.* Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479. Springer, Berlin, Heidelberg. 2009

[8] Pasalic, E.; *On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers*; IEEE Transactions on Information Theory. Vol. 55 Ed.7º, 2009.

[9] Biryukov A., Shamir A. (2000) Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. In: Okamoto T. (eds) Advances in Cryptology — ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976. Springer, Berlin, Heidelberg.

[10] http://evc.cin.edu.ar/informacion consultada el 23/2/2018.